

United States Northern District of Mississippi – MSND and MSNP

Information Technology Appropriate Use and Security Policy & Agreement

Revised 07/09/2019

Contents

Contents.....	2
Revision Log	3
Overview	4
Guidance.....	4
Definition of IT Assets	4
Annual Awareness Training	5
Appropriate Business Use.....	6
Appropriate Personal Use	6
Inappropriate Use.....	7
Usage Policies by System.....	8
E-Mail.....	8
Instant Messaging.....	8
Internet & Social Media.....	8
Voice Mail	9
DCN Network (Wired and Wireless)	9
Software.....	9
VPN (Remote Access)	9
Mobile Devices	10
Password Policy	10
Data Protection	10
Physical Protection.....	10
Security Incident Procedure	11

Revision Log

Date	Description	Editor
09/26/2017	Initial Policy	Kevin Helton
11/06/2017	Initial Policy Updates	Kevin Helton
11/16/2017	Changed Revision Date	Kevin Helton
12/14/2018	Reviewed	Don Conrad
05/31/2019	Reviewed and Updated	Roy Geoghegan
07/09/2019	Incorporated feedback from Judge Brown	Roy Geoghegan

Overview

This document outlines the appropriate use of Information Technology (IT) assets and the security requirements of IT asset users, as mandated by the 2019 Guide to Judiciary Policy, Volume 11: Internal Control - Chapter 6: Information Systems and Security and Volume 15: Information Technology.

Links to reference documents are defined where appropriate. Unless otherwise stated, all references are to the specified volume of the Guide to Judiciary Policy.

Guidance

According to the Guide to Judiciary Policy, policies and procedures must be developed for appropriate use of judiciary computer systems [Volume 15 § 310.20.10 (e) (3)]. Employees are responsible for the proper use of, and security measures for, government computers and the automated systems and records at their disposal. [Volume 11 § 250.60 (b)]. The MSND/MSNP policies for these requirements, including this document, are:

- MSND/MSNP Access Control Policy
- MSND/MSNP Information Technology Awareness and Training Policy
- MSND/MSNP Backup, Storage, and Recovery Policy
- MSND/MSNP Configuration Management Policy
- MSND/MSNP Contingency Planning and Disaster Recovery Policy
- MSND/MSNP Incident Response Plan
- MSND/MSNP Log Management Policy
- MSND/MSNP Maintenance Policy
- MSND/MSNP Media Sanitization and Information Disposal Policy
- MSND/MSNP Network Management Policy
- MSND/MSNP Password Security Policy
- MSND/MSNP Patch Management Policy
- MSND/MSNP Information Technology Physical Security Policy
- MSND/MSNP Information Technology Exceptions Policy
- MSND/MSNP Remote Access Policy
- MSND/MSNP Witness Protection Policy
- MSND/MSNP Wireless Local Area Network Policy
- MSND/MSNP Foreign Travel Policy

Definition of IT Assets

The IT assets covered by this policy are defined in [Volume 15, § 310.10.10] as including:

- Networks and their infrastructure (e.g., servers, switches, cables, firewalls):
 - the judiciary's wide-area networks (WAN) (e.g., the Data Communications Network (DCN), Public Access to Court Electronic Records (PACER-Net), and Defender Services (DWAN));
 - judiciary local area networks (LANs);
 - judiciary-provided private and public wireless networks;
 - courtroom IT systems; and

- phone systems.
- Devices and equipment owned by the judiciary that do not connect to judiciary systems or networks (e.g., information systems used in support of WITSEC).
- Devices and equipment forming or connected to judiciary systems:
 - judiciary-owned workstation computers and peripherals (e.g., printers, copiers, phones, fax machines);
 - judiciary-owned portable computers and other mobile devices (e.g., laptops, tablets, smart phones, cell phones);
 - digital media (including internal and external hard drives, USB drives, CDs, DVDs, and tapes); and
 - supporting systems (e.g., power supply, HVAC systems in IT closets and facilities, communications connections).
- Software residing on judiciary systems, whether judiciary-developed (e.g., CM/ECF) or commercial (e.g., MS Word, Lotus Notes).
- Judiciary applications and their associated information that are maintained on privately owned computers and mobile devices.
- Data and information:
 - data and information maintained on judiciary systems and devices, including information available to the public on judiciary systems (e.g., CM/ECF, the judiciary's websites, public kiosks);
 - judiciary data and information on third-party systems by judiciary contract or other formal agreement (e.g., backup sites, alternate sites);
 - judiciary data and information on the privately owned devices of users; and
 - sensitive judiciary information, such as payroll records, contract files, etc.

Annual Awareness Training

All judiciary employees must be properly trained via annual IT security awareness training regarding local and national information security policies [Volume 15 § 340, and Volume 11 § 650 (b)].

This policy will be reviewed and updated annually [Volume 11 § 630].

Appropriate Business Use

- I understand that government-owned equipment is for the use of judiciary employees in their performance of official government business [Volume 15 § 525 (b)].
- I will adhere to the Code of Conduct when using judiciary computer systems [Volume 15 § 525.40 (c), Volume 15 § 525.50, and Volume 2 Part A, Chapter 3].
- I understand that upon logging on to court systems, and before being allowed access to any system and/or network resources, I will be required to consent to monitoring of my use by accepting the language in this banner: [Volume 15 § 515.30].

United States District Court and Probation Office - Northern District of Mississippi

NOTICE TO USERS - Monitoring/Security Warning

This is a U.S. Government system. Unauthorized entry into or use of this system is prohibited and subject to prosecution under Title 18 of the U.S. Code or other sanctions. All activities and access attempts are logged. All data on or replicated from this system may be reviewed in accordance with Judiciary policies. DO NOT LOG IN if you do not agree to these conditions.

Appropriate Personal Use

Personal use of government-owned equipment is defined as "activity conducted by employees for purposes other than official government business" [Volume 15 § 525.30] and is not deemed inappropriate personal use [Volume 15 § 525.50] when it occurs within the parameters below:

- I understand that as a Judiciary employee, I am permitted limited use of government-owned equipment for personal needs if such use does not interfere with official business and involves minimal additional expense* to the government [Volume 15 § 525.20 (a)].
 - * Minimal additional expense is defined as "personal use that will result in no more than normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Examples of such minimal additional expenses include: making a limited number of photocopies, using a computer printer to print a limited number of pages, making occasional phone calls, infrequently sending e-mail messages, and limited use of the internet" [Volume 15 § 525.30].
- I understand that limited personal use of government-owned equipment should only occur during non-work time** and that this privilege to use government-owned equipment for non-government purposes may be revoked or limited at any time by appropriate judiciary officials [Volume 15 § 525.20 (b-c)].
 - ** Employee Non-Work Time is defined as "time when employees are not otherwise expected to be addressing official business, such as: off-duty hours before or after a workday, lunch periods or other authorized breaks, or weekends or holidays" [Volume 15 § 525.30].
- I understand that as a judiciary employee I may, for example, use government-owned equipment to review Thrift Savings Plan accounts, monitor medical, dependent care, or

commuter benefit reimbursement accounts, seek employment, or communicate with volunteer charity organizations [Volume 15 § 525.40 (a)].

- I understand that I must, at all times when using government-owned equipment for limited personal purposes, avoid giving the impression that I am acting in an official capacity. If there is a potential that such limited personal use could be interpreted to represent official business of the judiciary, I will use an adequate disclaimer, such as, "The contents of this message are personal and do not reflect any position of the judiciary or the court unit" [Volume 15 § 525.40 (b)].

Inappropriate Use

- I will not attempt to gain unauthorized access to other systems [Volume 15 § 525.50 (b)].
- I will not create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of subject matter [Volume 15 § 525.50 (c)].
- I will not use equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public, such as hate speech, or material that ridicules others on the basis of race, creed, religion, color, gender, disability, national origin, or sexual orientation [Volume 15 § 525.50 (d)].
- I will not create, download, view, store, copy, transmit, or retransmit sexually explicit or sexually oriented material [Volume 15 § 525.50 (e)].
- I will not create, download, view, store, copy, transmit, or retransmit material related to illegal gambling, illegal weapons, terrorist activities, and any other illegal or prohibited activities [Volume 15 § 525.50 (f)].
- I will not use equipment for commercial activities or in support of commercial activities or in support of outside employment or business activity, such as: consulting for pay, administering business transactions, or selling goods or services [Volume 15 § 525.50 (g)].
- I will not use equipment for fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity [Volume 15 § 525.50 (h)].
- I will not use equipment in a manner that results in loss of productivity, interference with official duties, or greater than minimal additional expense to the government [Volume 15 § 525.50 (j)].
- I will not acquire, use, reproduce, transmit, or distribute without authorization any controlled information such as judiciary sensitive data, proprietary data subject to the intellectual property rights of others, such as copyright, trademark or other rights (beyond fair use), as well as computer software and data (e.g., export controlled software or data) [Volume 15 § 525.50 (k)].
- I will not use judiciary-provided access to online investigative tools and databases*** containing personal information to gather information for non-work-related purposes, including attempting to research friends, neighbors, acquaintances, celebrities, other public figures, etc. [Volume 15 § 525.50 (l)].

*** Online investigative tools include LexisNexis and Westlaw public records or other databases that contain personal information (e.g., telephone, driver's license,

auto registration and VIN numbers, home addresses, property ownership records, voting records) [Volume 15 § 525.50 (l)].

Usage Policies by System

E-Mail

- I will not use my court provided email address for anything other than official government business. This includes making purchases (e.g., Amazon, eBay), using online services (e.g., social networking, blogging), and personal account access (e.g., banking, utilities). I understand this could result in massive amounts of junk/spam mail to be sent to me.
- I understand that sending judiciary information through personal web e-mail accounts outside the judiciary network is discouraged because the email accounts do not afford sufficient security or privacy [Volume 15 § 330.50 (b)].

Instant Messaging

- I will only use the instant messenger (IM) program provided by the court [Volume 15 § 330.40 (a)].

Internet & Social Media

- I understand that my Internet access will be restricted according to my court unit's specific internet access/blocking settings [Volume 11 § 660 (b)].
- I will use discretion and avoid accessing internet sites that may be inappropriate or reflect badly on the judiciary [Volume 15 § 510.30 (b)(1)].
- I will not use applications that employ peer-to-peer file sharing, chat rooms, or IM (other than provided by the court) for communicating outside the DCN. I understand that these applications pose extraordinary security risks to the judiciary's information technology infrastructure and can be blocked at the internet gateways until the security risks posed by their use can be mitigated. Examples of peer-to-peer applications are Skype, Facetime, Napster, BitTorrent, and GoogleTalk, among others [Volume 15 § 330.40 (b)].
- I understand that access to personal web e-mail accounts (e.g., AOL Mail, Gmail, Outlook, and Yahoo) from within the DCN is strongly discouraged. Use of these accounts poses threats to the judiciary's IT infrastructure because web email messages and their attachments bypass the existing network antivirus protections in place at the internet gateways and on the courts' email servers [Volume 15 § 330.50 (a)].
- I will not identify myself or others as court employees when using non-court messaging services (instant messaging, social networks, blogging, etc.). My actions on these networks/services may be viewed as official business by other users. If there is a potential that such limited, appropriate, personal use could be interpreted to represent official business of the judiciary, an adequate disclaimer must be used, such as, "The contents of this message are personal and do not reflect any position of the judiciary or the United States Probation Office for the Northern District of Mississippi" [Volume 15 § 525.40 (b)].
- I will not post judiciary information to external news groups, bulletin boards, or other public sites without authority, including any use that could create the perception that the communication was made in an official capacity as a judiciary employee [Volume 15 §

525.50 (i)].

- I understand that as a court employee, I have a responsibility to prevent personal information about judges and sensitive court data from appearing on public sites [Volume 15 § 510.30 (c)].
- I have read and agreed to follow the Social Media Policy for the Northern District of Mississippi.

Voice Mail

- I will carefully safeguard my voicemail PIN [Volume 15 § 330.80(f-g)].
- I will protect my voice mail from unauthorized access (e.g., to be used to make fraudulent calls or to obtain sensitive judiciary information) [Volume 15 § 330.80].
- I will not leave voice mail messages containing sensitive information (e.g., credit card numbers, procurement decisions) [Volume 15 § 330.80 (g)].

DCN Network (Wired and Wireless)

- I will not use the network in a way that could cause congestion, delay, or disruption of service to any government system, including, but not limited to, use of electronic greeting cards, video, sound, or other large file attachments, "push" technology on the internet, and other continuous data stream uses [Volume 15 § 525.50(a)].
- I will not connect any personal software or equipment to the court's wired or wireless networks without specific authorization from my judge or the Clerk of Court [Volume 15 § 530.20.10].
- I will not connect any personal Wi-Fi equipment to the wired private judiciary network [Volume 15 § 330.70.15].

Software

- I understand that I am not allowed to install personally-owned software on court-issued desktops and laptops. If I need software installed, I will obtain written approval from my Judicial Officer, Clerk of Court, or Chief U.S. Probation Officer; contact IT staff for installation; provide the software and license information to IT staff for a security risk review; and obtain approval by the IT Security Officer. Installation of the software will be performed by the IT staff [Volume 15 § 535.30 (d)].
- I will allow IT staff to perform routine security-related maintenance, including the installation and continued updates of client software, anti-virus software, firewall products, operating system patches, third-party software patches, and firmware updates [Volume 15 § 330.60.60 (b)].

VPN (Remote Access)

- I understand that VPN and Remote Access technologies are provided to secure access to judiciary networks from remote locations and to extend the judiciary network beyond the wired courthouse and judiciary office locations. I will only use these technologies to perform approved work-related activities or job duties on judiciary or employee-owned computers [Volume 15 § 330.60.10, and Volume 15 § 330.60.50 (b)].
- I understand that anti-virus software is mandatory on all computers that access judiciary networks [Volume 15 § 330.25].

- I understand that if I do not maintain adequate security safeguards, remote access privileges may be suspended or terminated [Volume 15 § 330.60.80 (c)].
- I understand that personally-owned computers are not to be used to access (via VPN, Remote Access, or WiFi) judiciary networks.
- I understand the court is not liable for damage to personal or real property, any operating or service costs, or repair, when using personal equipment for conducting court business.

Mobile Devices

- I understand that personally-acquired applications may be installed on government owned mobile devices (iPad or iPhone), if such personally-acquired applications do not detrimentally impact the performance or security of the court-owned device. I understand I will not be reimbursed for any personally-acquired applications, unless preauthorized for official use [Volume 15 § 570 (e)].
- I understand that any installed personally-owned applications on court devices may be removed during updates, applying security settings, or by unit device management policies. Ownership rights to these applications are abandoned upon return or disposal of the court-issued device [Volume 15 § 570 (e-f)].
- I will not use Peer-to-Peer applications while the mobile device is connected to the DCN (via VPN). Examples of peer-to-peer applications are Skype, Facetime, Napster, BitTorrent, and GoogleTalk, among others [Volume 15 § 330.40].
- I understand the IT Department will not support personally-owned devices.

Password Policy

- I understand that as a user of judiciary information systems, I am responsible for creating, protecting, and securely managing passwords [Volume 15 § 390 (a)].
- I understand that my password will be changed periodically per system requirements (on applicable systems) [Volume 15 § 390 (b)(1)].
- I will carefully safeguard my passwords. I will not share my passwords or give them to family members or friends [Volume 15 § 330.60.60 (c)].
- I understand that the IT Department may need to know my password for support or maintenance reasons.
- I will use password-protected screensavers that automatically activate after a period of inactivity to prevent unauthorized system access to my computer [Volume 11 § 660 (f)].

Data Protection

- I will protect non-public judiciary information from unauthorized disclosure. Such information includes, but is not limited to, chambers work product, warrants, sealed cases, investigative information, budget and accounting material, and personnel data (e.g., personal information about judiciary personnel, payroll, etc.) [Volume 15 § 310.10.20 (a), and Volume 11 § 660 (g)].
- I will ensure that important data is stored on network drives and not on desktop or laptop hard drives, so that the data is properly backed up.

Physical Protection

- I will physically protect and secure equipment, devices, media, and printed output against

loss, theft, and misuse, [Volume 11 § 650 (b)(5)] and from observation by unauthorized individuals [Volume 15 § 310.10.30 (b)(1)].

- My court-issued laptop and/or mobile devices will be kept in a secure location when traveling and when not in use. I will not check a court-issued technology device when traveling by commercial carrier [MSND/MSNP Cybersecurity for International Travel Policy].
- I will not modify equipment (physically or functionally) without approval from the IT Department, including loading personal software or making configuration changes [Volume 15 § 525.35 (b)].
- I will physically protect my equipment from damage by food, liquids, cleaning products, hygiene products, dirt, dust, magnets, extreme temperatures, prolonged exposure to sunlight, or pets.
- I will return, in good condition, all equipment checked out to me, including removable media (such as USB flash drives, external hard drives, etc.), to the court when these devices are either no longer needed or at the end of my employment in accordance with the applicable Property Pass [AO 566] or Property Caretaker Receipt [AO 563].

Security Incident Procedure

A security incident is defined as "any real or suspected adverse event impacting the security of computer systems or networks. These include, but are not limited to: attempts to gain unauthorized access to a system or its data; unwanted disruption or denial of service; unauthorized use of a system for processing, accessing, or storing data; and changes to system hardware, firmware, or software characteristics without the owner's consent" [Volume 15 § 320.20 (a)].

The **IT Security Officer** is the designated contact at each judicial district responsible for implementing security policies and procedures within their court, addressing security threats directed against IT assets within the court unit system boundary, and reporting all critical and serious incidents to the Judiciary Automated Systems Incident Response Capability (JASIRC) [Volume 15 § 310.20.05 (b), and Volume 15 § 320.20 (d)].

IT Security Officer: Roy Geoghegan
Email: Roy_Geoghegan@msnd.uscourts.gov
Office: (662)281-3034
Cell: (662)816-1287

I understand that it is my responsibility to IMMEDIATELY contact the IT Security Officer and my supervisor for any of the following reasons:

- Any suspected security incident [Volume 11 § 650 (b)(4)].
- Any suspected or actual compromise of a password [Volume 15 § 390(c)].
- Any suspected voice mail fraud or voice mail PIN compromise [Volume 15 § 330.80 (k)].
- Any suspected attempt at unauthorized access, or if I suspect I am the target of an attempted exploitation.
- Any suspected disclosures of restricted information or data.
- Any loss of court-issued equipment. I understand that if court-issued equipment has been

lost, I am responsible for providing a written statement of the details surrounding the loss to the IT Security Officer and my supervisor.

- Any theft of court-issued equipment. I understand that if court issued equipment has been stolen from me, I am responsible for providing a police report and written statement of the details surrounding the incident to the IT Security Officer and my supervisor. For theft within the court, the U.S. Marshals Service must also be notified.
- Any loss or theft of **personally-owned mobile devices** configured for use with court services (such as Traveler, Airwatch, etc.). I understand that the IT Department will initiate a process to remotely delete all data or wipe the entire device.

Information Technology Appropriate Use and Security Agreement

By signing this agreement:

- I acknowledge that I have read this Information Technology Appropriate Use and Security Policy. I agree to appropriately use government IT assets and abide by the policy's provisions. I also acknowledge that I understand my security responsibilities as a user of government IT assets [Volume 15 § 330.60.70, and Volume 15 § 510.10 (c)].
- I understand that unauthorized or improper use of government IT assets may result in loss of the privilege, limitation of the privilege, disciplinary or adverse actions, criminal penalties, and/or civil penalties, including financial responsibility for the costs of improper use [Volume 15 § 525.60, and Volume 15 § 510.20 (c)].
- I understand that use of government assets is monitored and may be reported to the employee's court unit upon request. This monitoring includes but is not limited to internet usage, email usage, etc. [Volume 15 § 510.20 (d)].

Date

Signature of Employee

Printed Name of Employee